Worldwide Threat Assessment of the U.S. Intelligence Community
Daniel R. Coats, Director of National Intelligence
Senate Select Committee on Intelligence, January 29, 2019

This summary of the cyber highlights was produced by the MS-ISAC for your situational awareness. It is not a complete summary of DNI Coats' statement for the record and we strongly recommend that MS-ISAC members read the full statement.

Statement for the Record

Cyber Threat

- Adversaries and strategic competitors will increasingly use cyber capabilities to seek political, economic, and military advantage over the United States and its allies and partners.
- At present, China and Russia pose the greatest espionage and cyber threats, but all adversaries and strategic competitors will increasingly build and integrate cyber espionage, attack, and influence capabilities into their efforts to influence U.S. policies and advance their own national security interests.
- The growing availability and use of publicly and commercially available cyber tools is increasing the overall volume of unattributed cyber activity around the world.

Cyber Threat Actors

- Russia
    - Russia poses a cyber espionage, influence, and attack threat to the United States and our allies.
    - Russia continues to be a highly capable and effective adversary, integrating cyber espionage, attack, and influence operations to achieve its political and military objectives.
    - Russia is now staging cyber attack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis and poses a significant cyber influence threat.
    - Russian intelligence and security services will continue targeting US information systems, as well as the networks of allies for technical information, military plans, and insight into government policies.
    - Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure while mapping our critical infrastructure with the long-term goal of being able to cause substantial damage.
- China
    - China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems.
    - China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies.
    - China will authorize cyber espionage against key U.S. technology sectors when doing so addresses a significant national security or economic goal not achievable through other means.
    - China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure in the U.S.
- Iran
    - Iran continues to present a cyber espionage and attack threat.
    - Iranian cyber actors are targeting U.S. government officials, organizations, and companies to gain intelligence and position themselves for future cyber operations.

    - Iran has been preparing for cyber attacks against the United States and our allies. It is capable of causing localized, temporary disruptive effects.
- North Korea
    - North Korea poses a significant cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks.
- Criminals
    - Foreign cyber criminals will continue to conduct for-profit, cyber-enabled theft and extortion against U.S. networks.
- Terrorists
    - Terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, and they may use such disclosures to coerce, extort, or to inspire and enable physical attacks against their victims.

Online Influence Operations and Election Interference

- U.S. adversaries and strategic competitors probably already are looking to the 2020 U.S. elections as an opportunity to advance their interests.
- U.S. adversaries and strategic competitors almost certainly will use online influence operations to try to weaken democratic institutions, undermine U.S. alliances and partnerships, and shape policy outcomes in the U.S. and elsewhere.
- Russia's social media efforts will continue to focus on aggravating social and racial tensions, undermining trust in authorities, and criticizing perceived anti-Russia politicians.
- China is expanding its ability to shape information and discourse relating to China abroad, especially on issues that China views as core to party legitimacy, such as Taiwan, Tibet, and human rights.
- Iran will continue to use online influence operations to try to advance its interests.
- Adversaries and strategic competitors probably will attempt to use deep fakes or similar machine-learning technologies to create convincing—but false—image, audio, and video files to augment influence campaigns directed against the United States and our allies and partners.
- Adversaries and strategic competitors also may seek to use cyber means to directly manipulate or disrupt election systems, such as by tampering with voter registration or disrupting the vote tallying process, either to alter data or to call into question our voting process.

Counterintelligence

- Geopolitical, societal, and technological changes will increase opportunities for foreign 14 intelligence services and other entities—such as terrorists, criminals, and cyber actors—to collect on US activities and information to the detriment of US interests.
- Nonstate Actors
    - Nonstate actors, including hacktivist groups, transnational criminals, and terrorist groups, will attempt to gain access to classified information to support their objectives. They will use human, technical, and cyber means to perform their illicit activities and avoid detection and capture.